(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4531211号
(P4531211)

(45)発行日　平成22年8月25日(2010.8.25)　(24)登録日　平成22年6月18日(2010.6.18)

(51)Int.Cl.		F I		
E05B 49/00	(2006.01)	E05B	49/00	K
E05B 19/00	(2006.01)	E05B	49/00	B
E05B 35/12	(2006.01)	E05B	49/00	F
E05B 47/00	(2006.01)	E05B	49/00	J
		E05B	49/00	R

請求項の数 8　(全 23 頁)　最終頁に続く

(21)出願番号　特願2000-204259 (P2000-204259)
(22)出願日　平成12年7月5日 (2000.7.5)
(65)公開番号　特開2002-21385 (P2002-21385A)
(43)公開日　平成14年1月23日 (2002.1.23)
審査請求日　平成19年5月24日 (2007.5.24)

(73)特許権者　000202361
綜合警備保障株式会社
東京都港区元赤坂１丁目６番６号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　長須賀　卓
東京都港区元赤坂１丁目６番６号　綜合警備保障株式会社内
(72)発明者　大▲崎▼　摩耶
東京都港区元赤坂１丁目６番６号　綜合警備保障株式会社内

審査官　深田　高義

最終頁に続く

(54)【発明の名称】マスターキー機能を有する携帯端末およびそれに用いられる電気錠

(57)【特許請求の範囲】
【請求項１】
監視センタとの通信により警備対象の建物の錠を施解錠するための鍵データを受信する受信部と、
前記受信部において受信された鍵データを記憶する記憶部と、
前記鍵データをもとに施解錠する錠に対して施解錠信号を出力する施解錠信号出力部と、
錠を施解錠するための操作を行なう操作部と、
前記操作部の操作により前記記憶部に記憶された鍵データをもとに前記施解錠信号出力部から施解錠信号を出力させる制御部と、
分解されたことを検知して前記鍵データを消去する耐タンパ手段と、
を有し、
前記鍵データは、施開錠の対象となる鍵の錠前情報と、施開錠の対象となる鍵の種類を示す情報と、鍵データの消去条件を示す情報含むことを特徴とする携帯端末。
【請求項２】
前記鍵データをもとに施解錠操作に必要な情報を表示する表示部を有し、前記操作部の操作により前記記憶部に記憶された鍵データをもとに表示部による表示を行なわせ、または施解錠信号出力部から施解錠信号を出力させる制御部と有することを特徴とする請求項１に記載の携帯端末。
【請求項３】

警備対象の建物の錠を施解錠するための鍵データとして監視センタから受け取った暗号化コードを入力する操作と錠を施解錠するための操作を行なう操作部と、
前記操作部から入力された鍵データを記憶する記憶部と、
前記鍵データをもとに施解錠する錠に対して施解錠信号を送信する施解錠信号出力部と、
前記操作部の操作により前記記憶部に記憶された暗号化された鍵データを復号して前記施解錠信号出力部から施解錠信号を送信させる制御部と、
分解されたことを検知して前記鍵データを消去する耐タンパ手段とを有し、
前記鍵データは、施開錠の対象となる鍵の錠前情報と、施開錠の対象となる鍵の種類を示す情報と、鍵データの消去条件を示す情報含むことを特徴とする携帯端末。

【請求項４】
警備対象の建物の錠を施解錠するための鍵データとして監視センタから受け取った暗号化コードを入力する操作と錠を施解錠するための操作を行なう操作部と、
前記操作部から入力された鍵データを記憶する記憶部と、
前記鍵データをもとに施解錠操作に必要な情報を表示する表示部と、
前記鍵データをもとに施解錠する錠に対して施解錠信号を送信する施解錠信号出力部と、
前記操作部の操作により前記記憶部に記憶された鍵データを復号して表示部による表示を行なわせ、または施解錠信号出力部から施解錠信号を出力させる制御部と、
分解されたことを検知して前記鍵データを消去する耐タンパ手段とを有し、
前記鍵データは、施開錠の対象となる鍵の錠前情報と、施開錠の対象となる鍵の種類を示す情報と、鍵データの消去条件を示す情報含むことを有することを特徴とする携帯端末。

【請求項５】
前記携帯端末が監視センタから鍵データを受信する際または錠を施解錠する際、該携帯端末の使用者が該携帯端末を使用する正当な権限を有する者であるか否かを確認するための認証部を設けたことを特徴とする請求項１乃至４記載の携帯端末。

【請求項６】
前記携帯端末は、施解錠する対象となる錠の種類に応じて異なる形式で施解錠信号を出力するアダプタを備えたことを特徴とする請求項１乃至５記載の携帯端末。

【請求項７】
回転軸の両端に取り付けられた外部ドアノブと、内部ドアノブと、回転軸の回転により扉の端面より出入りするデッドボルトと、前記外部ドアノブに設けられ鍵が挿入されるシリンダ部を有するシリンダ鍵に取り付けられ、携帯端末から出力される施解錠信号により施解錠される電気錠であって、電気錠を動作させるための電力供給を前記携帯端末から受ける給電部と、前記給電部から供給される電力により動作し、電気錠制御部の制御により錠を施解錠する駆動部と、前記携帯端末からの施解錠信号により前記駆動部を制御して錠を施解錠する電気錠制御部と、から構成され、
前記駆動部は、モータと、前記シリンダ錠の回転軸に連結されるリンク機構と、前記モータの回転をリンク機構に伝達するギア機構とから構成されることを特徴とする電気錠。

【請求項８】
前記リンク機構と前記ギア機構との間に、前記回転軸の回転が前記モータに伝達されることを遮断する遊びが設けられていることを特徴とする請求項７記載の電気錠。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、錠を施解錠するために用いるキー機能を有する携帯端末に関し、特に、異なる錠を施解錠することができるマスターキーの機能を有する携帯端末に関する。

【０００２】
【従来の技術】

一般的な機械警備システムは、警備対象である契約先の建物または住居に侵入者や火災などの異常事態を検知するセンサおよび通報装置を設置し、夜間や休日などの無人となった建物または住人が外出して不在となった住居の警備を行なう。

【０００３】

前記センサが異常事態を検知すると、通報装置により電話回線等を介して警備会社の監視センタに異常事態を検知した旨の通報が行なわれる。

【０００４】

警備会社の監視センタでは、前記通報を受けると、当該建物または住居に警備員を派遣し、状況の確認を行なわせるとともに、必要に応じて警察や消防など関係機関への出動要請なども行なう。

【０００５】

現場に派遣された警備員は、事前に契約先から借り受けていた鍵を使用して建物内または住居内に入り、前記センサにより検知された異常の原因を究明する。

また、確認された異常の状況に応じて事態の収拾にあたり、あるいは、被害の拡大防止のために必要な対処を行なう。

【０００６】

【発明が解決しようとする課題】

ところが、前記契約先の建物または住居に入るための鍵に関し、以下に示す問題点及び改善すべき課題が存在した。

【０００７】

（１）前記借り受けた鍵は、専用の鍵箱に収納し、その鍵箱を警備員の待機場所に保管するか、当該地区を担当する警備員の警備車両に載せるが、鍵の数が増加するにつれて保管場所の確保が困難になる。

【０００８】

（２）それぞれの警備員は担当地区が割り当てられており、異常事態が検知された際、当該地区を担当する警備員が派遣される。ところが、当該地区を担当する警備員が別件対応中などのため現場に向かうことができない場合、隣接する地区を担当する警備員を代わりに派遣しなければならない。このとき、隣接する地区を担当する警備員は当該地区の契約先の鍵を所持していないため、当該地区を担当する警備員と任意の場所で合流し、鍵の受け渡しを行なわなければならなかった。

【０００９】

また、契約先の鍵を警備員の待機場所に保管している場合、当該地区を担当する警備員が出動中のとき、または隣接する地区を担当する警備員が代わりに派遣されるとき、いずれも当該地区の待機場所に寄ってから現場に向かわなければならなかった。

【００１０】

よって、鍵の受け渡しを行なうために、現場に向かうまでの時間をロスしていた。

【００１１】

この状況を図1を用いて更に説明する。

【００１２】

図示する通り、警備員ａ～警備員ｄの担当地区がＡ地区～Ｄ地区として割り当てられており、各警備員はそれぞれの地区の待機場所で待機している。また、各地区の契約先建物に入るための鍵は、それぞれの地区の警備員が保管している。

Ａ地区の契約先A1において異常事態が検知されると、監視センタからの指示により警備員ａは契約先A1に派遣され、状況確認などの対応を行なう。

【００１３】

このとき、Ａ地区の契約先A2において異常事態が検知されると、本来は警備員ａが契約先A2に派遣されるが、契約先A1に出動中であるため対応できない。

【００１４】

そこで、隣接地区であるＣ地区の警備員ｃが契約先A2に派遣されるが、警備員ｃはＡ地区の契約先の鍵を持っていないため、警備員ａと合流してから契約先A2に向かうか、待機場

所Ａに寄ってから契約先A2に向かうため、直接契約先A2に向かう場合と比較して大きく迂回することになる。

【００１５】

そのため、現場に到着するまでの時間が余計にかかっていた。

【００１６】

（３）契約先において異常事態が検知され、警備員が状況確認のために建物内に入る場合の他、契約先に設置したセンサ等の警備用の機器が正常に機能するよう、保守要員が点検作業や交換作業のために契約先の建物内に入る場合にも契約先から借り受けた鍵が使用される。

【００１７】

このような場合においても、当該地区を担当する警備員と保守要員との間で鍵の受け渡しを行なわなければならず、時間の無駄が生ずるとともに煩わしかった。

【００１８】

（４）前記（２）、（３）における鍵の受け渡しを行なわなくても済むように、予め鍵を複製しておき、当該地区を担当する警備員および隣接する地区を担当する警備員に渡しておくことも考えられるが、各警備員が保管する鍵の数が大幅に増加する、鍵の数が増えるにつれて盗難や紛失などが発生する危険性が増す、契約先の多くは鍵を複製されることに対して抵抗がある、などの理由により実施できなかった。

【００１９】

（５）ホテルなど部屋数の多い建物においては、多数の鍵を持ち歩かなくても済むようにするための手段として、マスターキー方式が採用されている。マスターキー方式は、マスターキーを用いて複数の錠を施解錠するようにした方式である。この方式を適用すれば、警備員が保管しなければならない鍵の数を削減できる。

【００２０】

ところが、従来のマスターキー方式は、マスターキーを紛失したり盗難されたりした場合、他人に悪用されるおそれがあった。万が一、このような事態が発生すると、マスターキーに対応する錠を全て交換するなどの必要があり、多大な費用および労力を要した。

【００２１】

そのため、警備員が複数の契約先の建物に入館するための鍵として、従来のマスターキー方式を安易に導入するわけにはいかなかった。

【００２２】

（６）警備員が保管する鍵の数を削減するために、契約先建物の出入口等に使用される錠を電気錠に交換し、暗証番号等により施解錠できるようにすることも考えられるが、電気錠自体高価であること、後から電気錠を設置する場合、電源を確保するために配線工事を行なう必要があり工事費が高くなるなどの理由から、容易に電気錠を設置することはできなかった。

【００２３】

（７）契約先の建物に使われている錠は、シリンダ式のもの、テンキー（暗証番号）を用いるもの、磁気カードなどのＩＤカードを用いるものなど、様々な種類があり、各警備員の担当している地区には、これらの錠が混在している。

【００２４】

したがって、警備員が保管する鍵の数を削減しようとする場合において、理想的には、異なる種類の錠が存在する場合でも対応できるようにする手段が必要である。

【００２５】

本発明は、上記問題点を解決するためになされたものであり、警備員が契約先の鍵を多数保管しなくても済み、また警備員同士で鍵の受け渡しを行なわなくても済むようにするキーの機能を有する携帯端末の提供を目的とする。

また、キーの機能を有する携帯端末について、万が一、携帯端末が盗難や紛失にあっても、正当な権限を持たない者は使用できないようにし、悪用されるのを防止することを目的とする。

【００２６】
さらには、異なる種類の錠を施解錠できるようにし、汎用性の高いマスターキーとして使用できる携帯端末の提供を目的とする。
【００２７】
【課題を解決するための手段】
請求項１の発明は、監視センタとの通信により錠を施解錠するための鍵データを受信する受信部と、前記受信部において受信された鍵データを記憶する記憶部と、前記鍵データをもとに施解錠する錠に対して施解錠信号を出力する施解錠信号出力部と、錠を施解錠するための操作を行なう操作部と、前記操作部の操作により前記記憶部に記憶された鍵データをもとに前記施解錠信号出力部から施解錠信号を出力させる制御部と
を有することを特徴とする携帯端末である。
【００２８】
本発明の携帯端末は、監視センタより送信された鍵データは受信部で受信され、記憶部に記憶される。そして、操作部を操作することより受信して記憶部に記憶された鍵データが施解錠信号出力部より出力され、対象とする錠を解錠する。請求項２の発明は、監視センタとの通信により錠を施解錠するための鍵データを受信する受信部と、前記受信部において受信された鍵データを記憶する記憶部と、前記鍵データをもとに施解錠操作に必要な情報を表示する表示部と、前記鍵データをもとに施解錠する錠に対して施解錠信号を送信する施解錠信号出力部と、錠を施解錠するための操作を行なう操作部と、前記操作部の操作により前記記憶部に記憶された鍵データをもとに表示部による表示を行なわせ、または施解錠信号出力部から施解錠信号を出力させる制御部とを有することを特徴とする携帯端末である。
【００２９】
請求項２の発明の携帯端末は、さらに、鍵データをもとに施解錠操作に必要な情報を表示する表示部を備える。施解錠信号出力部かたの施解錠信号による操作の他、この表示部に施解錠に必要な情報を表示させて施解錠を行なうことが可能となる。
【００３０】
請求項３の発明は、錠を施解錠するための鍵データとして監視センタから受け取った暗号化コードを入力する操作と錠を施解錠するための操作を行なう操作部と、前記操作部から入力された鍵データを記憶する記憶部と、前記鍵データをもとに施解錠する錠に対して施解錠信号を送信する施解錠信号出力部と、前記操作部の操作により前記記憶部に記憶された鍵データをもとに前記施解錠信号出力部から施解錠信号を送信させる制御部とを有することを特徴とする携帯端末である。
【００３１】
請求項３の発明の携帯端末は、錠を施解錠するための鍵データとして監視センタから受け取った暗号化コードを入力する操作を行なう操作手段を備えている。したがって、監視センタから、例えば、電話等による通信手段により受け取った暗号化された鍵データを入力することが可能となる。そして、入力した鍵データをもとに施解錠信号を施解錠信号出力部に出力させて施解錠を行なうことを可能とする。
【００３２】
請求項４の発明は、錠を施解錠するための鍵データとして監視センタから受け取った暗号化コードを入力する操作と錠を施解錠するための操作を行なう操作部と、前記操作部から入力された鍵データを記憶する記憶部と、前記鍵データをもとに施解錠操作に必要な情報を表示する表示部と、前記鍵データをもとに施解錠する錠に対して施解錠信号を送信する施解錠信号出力部と、前記操作部の操作により前記記憶部に記憶された鍵データをもとに表示部による表示を行なわせ、または施解錠信号出力部から施解錠信号を出力させる制御部とを有することを特徴とする携帯端末である。
【００３３】
請求項３の発明と同様、操作部を操作して鍵データを入力することが可能である。そして、入力した鍵データをもとに表示部に表示させるか、あるいは、施解錠信号を施解錠信号

出力部より出力させることにより施解錠を行なうことを可能とする。
【００３４】
請求項５の発明は、請求項１乃至４記載の携帯端末において、前記携帯端末が監視センタから鍵データを受信する際または錠を施解錠する際、該携帯端末の使用者が該携帯端末を使用する正当な権限を有する者であるか否かを確認するための認証部を設けたことを特徴とする。
【００３５】
請求項５の携帯端末は、使用者が正当な権限を有する者であるかどうかの確認が可能となり不正使用を防ぐことが可能となる。
【００３６】
請求項６の発明は、請求項１乃至５記載の携帯端末において、前記携帯端末は、施解錠する対象となる錠の種類に応じて異なる形式で施解錠信号を出力することを特徴とする。
【００３７】
請求項６の携帯端末は、一つの携帯端末で複数の形式の錠を施解錠することを可能とする。
【００３８】
請求項７の発明は、請求項１乃至５記載の携帯端末において、前記携帯端末は、施解錠する対象となる錠の種類に応じて異なる形式で施解錠信号を出力するアダプタを備えたことを特徴とする。
【００３９】
請求項７の携帯端末は、一つの携帯端末で複数の形式の錠を施解錠することを可能とする。
【００４０】
請求項８の発明は、携帯端末から出力される施解錠信号により施解錠される電気錠であって、電気錠を動作させるための電力供給を受ける給電部と、前記給電部から供給される電力により動作し、電気錠制御部の制御により錠を施解錠する駆動部と、前記携帯端末からの施解錠信号により前記駆動部を制御して錠を施解錠する電気錠制御部と、から構成されることを特徴とする電気錠である。
【００４１】
請求項８による電気錠は、本発明による携帯端末からの施解錠信号により作動し、携帯端末の機能を有効に利用することが可能となる。
請求項９の発明は、請求項８記載の電気錠において、前記駆動部は、モータと、シリンダ錠の回転軸に連結されるリンク機構と、前記モータの回転をリンク機構に伝達するギア機構とから構成され、前記リンク機構と前記ギア機構との間に、前記回転軸の回転が前記モータに伝達されることを遮断する遊びが設けられていることを特徴とする。
【００４２】
請求項９の発明の電気錠は、電気錠以外の手段、例えばキーをシリンダに挿入して錠を施解錠する場合、モータによる負荷がかかることを避けることが可能となる。
【００４３】
【発明の実施の形態】
本発明によるキー機能を有する携帯端末について説明する。
【００４４】
業務の流れについて
本発明による携帯端末が使用されるのは、主に、次の場合である。
機械警備システムを導入した契約先において、夜間や休日など契約先の者が不在となり警備状態に設定されているとき、センサにより異常事態が検知され監視センタに通報が行なわれたことにより、状況確認などのために警備員を派遣する場合。
【００４５】
機械警備システムを導入した契約先において、センサ等の警備用機器を定期的または要請により点検・交換するための保全作業を、契約先の者が不在となる夜間や休日に行なう場

合。
【００４６】
なお、契約先の者が立合いのもとで行なう保全作業の場合や、建物に管理人が常駐している場合など、既に解錠されており鍵が不要なときや、必要な鍵を現場で借り受けることができる状況であれば、本発明による携帯端末を用いる必要はない。
【００４７】
以下に、それぞれの場合について、概要を説明する。
【００４８】
異常事態の検知による対応の場合
次に図２に基づき、異常事態の検知による対応について説明する。図２において、警備対象である契約先建物Ａ１には機械警備装置を構成するセンサｓと通報装置Ｔ、出入口扉に設けられた錠ｋとその錠を施解錠する入力手段Ｒを備える。また、警備員ａ１は本発明による携帯端末１を持っている。
（ａ）異常事態の検知
契約先に設置したセンサｓが異常事態を検知すると、通報装置Ｔにより、監視センタ１００に対して異常事態を検知した旨の通報が行なわれる。
（ｂ）警備員に対する派遣指示
監視センタ１００は、前記通報を受けると、警備員ａ１に対し、無線や携帯電話を利用して現場に行き状況確認するよう派遣指示する。このとき、警備員ａ１の持つ携帯端末１に鍵データを送信する。
（ｃ）警備員による状況確認
警備員ａ１は、監視センタ１００からの指示により出動し、現場に到着すると、監視センタから送られた鍵データを利用し、携帯端末１により契約先建物の出入口等に設けられた錠ｋを解錠して中に入り、センサｓにより検知された異常事態の原因を確認する。また、確認された異常事態の原因に応じて、事態の収拾や被害の拡大防止など、必要な対応をとる。対応が完了すると、警備員は携帯端末１により錠ｋを施錠し、退出する。
【００４９】
保全作業の場合
次に、図３に基づき保守要員ｂ１が行なう保全作業の場合について説明する。
（ｄ）保全作業の発生
契約先建物Ａ１に設置したセンサｓや通報装置Ｔなどの警備用機器の故障により点検・交換を要請された場合、または警備用機器の定期点検等により、保守要員が契約先の建物に向かう場合、保守要員は監視センタ１００に作業連絡を入れ、契約先の建物に入館する旨を伝えるとともに鍵データの要求を行なう。
（ｅ）保守要員に対する鍵データの送信
前記契約先建物Ａ１に入館する旨の連絡および鍵データの要求を受けると、監視センタ１００は保守要員の持つ携帯端末１に鍵データを送信する。
（ｆ）保守要員による保全作業
保守要員ｂ１は、現場に到着すると、監視センタ１００から受け取った鍵データを利用し、携帯端末１により契約先建物の出入口に設けられた錠ｋを解錠して中に入り、センサ等の警備用機器の修理や点検などの保全作業を行なう。保全作業が完了すると、保守要員ｂ１は携帯端末１により錠ｋを施錠し、退出する。
【００５０】
現地において必要な鍵データのみを受け取る場合
次に、図４に基づき、他の手順として、警備員ａ１または保守要員ｂ１が契約先建物Ａ１に出動し、現場において監視センタ１００に必要な鍵データのみを要求し、送信してもらう場合について説明する。
（ｇ）警備員、保守要員の出動
契約先建物Ａ１に設置したセンサｓが異常事態を検知したことによる派遣指示、または警備用機器の点検等を要請されたことにより、警備員ａ１または保守要員ｂ１が現場に向か

う。なお、この時点では鍵データの送信は行なわれない。
（ｈ）錠のＩＤを取得
警備員または保守要員は、現場において施解錠する必要のある錠がある場合、錠の制御装置（図示せず）から携帯端末１に錠のＩＤを送信させ、あるいは錠に付与された識別番号を警備員または保守要員が確認して携帯端末１に入力し、施解錠する錠のＩＤを取得する。
（ｉ）錠データの要求、錠データの送信
（ｈ）において得られた錠のＩＤを監視センタ１００に送信し、施解錠するための鍵データを要求する。監視センタ１００では、要求に基づき、錠のＩＤに対応する錠データを送信する。
（ｊ）警備員、保守要員による対応
警備員ａ１または保守要員ｂ１は、監視センタ１００から受け取った鍵データを利用し、携帯端末１により契約先建物Ａ１に設けられた錠ｋを解錠して中に入り、それぞれ必要な対応をとり、作業が完了すると携帯端末１により錠ｋを施錠し、退出する。
【００５１】
なお、鍵データを要求する場合、監視センタ１００にいる監視員が直接対応するのでは、鍵データを送信するための手続きが監視員の負担になる恐れがある。
そこで、監視センタ１００に自動対応装置（図示せず）を設置し、警備員または保守要員が鍵データを要求する際、錠のＩＤなど識別情報を送ることにより、監視センタの自動対応装置が自動的に携帯端末に送信すべき鍵データを選択し、送信するようにすればよい。
【００５２】
認証の必要性について
前記業務の流れにおいて、監視センタから警備員または保守要員に対する鍵データの送信、携帯端末による契約先の出入口に設けられた錠の施解錠が行なわれている。
【００５３】
ここで、下記のような不正行為が想定されることから、不正行為を防止するための確認行為が必要となる。
【００５４】
前記（ｂ）、（ｅ）、（ｉ）における鍵データの送信の際、鍵データの不正入手および不正利用を防止するため、鍵データをどの携帯端末に送信したのか、鍵データを送信した際に携帯端末を使用していたのは誰であるかを確認しておく必要がある。
【００５５】
特に、（ｅ）、（ｉ）においては第三者が身分を偽って鍵データを要求してくることも考えられるため、正規の携帯端末であるか、携帯端末を使用する正当な権限を与えられた者であるかを確認することは重要である。
【００５６】
前記（ｃ）、（ｆ）、（ｊ）における錠を施解錠する際、不正な施解錠を防ぐため、正規の携帯端末であるか、携帯端末を使用する正当な権限を与えられた者であるかを確認する必要がある。
【００５７】
不正な施解錠としては、携帯端末と同等の機能を持つ不正な装置を製作して錠を施解錠する場合と、正規の携帯端末を第三者が強奪して不正使用する場合が考えられるので、これらの行為を防ぐための確認が重要である。
【００５８】
したがって、本発明による携帯端末を使用するにあたり、不正行為を防ぐための確認行為として認証を取り入れている。
【００５９】
なお、この認証は必須となる手順ではなく、監視センタから警備員に対して指示を与える際の手順や通信方式により、認証を行なうまでもなく相手方の確認が行なえる場合や、錠の種類により認証を取り入れても不正使用の防止効果を得られない場合は不要である。

【００６０】
携帯端末の構成
次に、本発明による携帯端末の実施例について説明する。図５は、本発明による携帯端末のブロック図を示し、（ａ）は第１の形態の携帯端末１及び（ｂ）は第２の実施携帯による携帯端末２を示す。なお、図５（ａ）の携帯端末１は、携帯端末と携帯電話の機能が一体化された場合の例を示し、図５（ｂ）の携帯端末２は携帯端末を携帯電話に接続して利用する場合の例を示している。図６は、図５（ａ）の携帯端末１と図５（ｂ）の携帯端末２のそれぞれの外観構成図を示している。
【００６１】
図５（ａ）の携帯端末１は、表示部１１、操作部１２、認証部１３、制御部１４、記憶部１５、送受信部１６、施解錠信号出力部１７、耐タンパ手段１８を備える。
【００６２】
なお、図５（ｂ）の携帯端末２は携帯端末１の送信部１６に代えて入出力部１９を備えている点で異なり他の構成は基本的に同じである。したがって、図５（ｂ）の場合、入出力部１９と携帯電話（無線機等）２０が図５（ａ）の送受信部１６に相当する。
【００６３】
表示部１１は、操作部１２を操作した際の入力確認、操作結果の確認など、各種情報を表示する。契約先建物の錠が暗証番号により施解錠するものである場合、暗証番号を表示させてもよい。
【００６４】
操作部１２は、警備員または保守要員が錠を施解錠するための操作、（必要に応じて）認証の際の暗証番号入力などを行なう。
【００６５】
認証部１３は、携帯端末１が鍵データを受信する際、または契約先に設けられた錠を施解錠するために使用される際、その使用者が携帯端末１を使用する正当な権限を与えられた者であるか否かを確認するための認証を行なう。認証の際は、暗証番号の入力や指紋照合、使用者が所有するＩＤカードを読み取るなど、既存の技術を適宜利用する。なお、指紋照合やＩＤカードを読み取る場合、指紋入力装置やカードリーダを携帯端末１に接続するか、その機能を携帯端末に設けるなどの必要がある。
【００６６】
制御部１４は、携帯端末１の各種制御を行なう。
【００６７】
記憶部１５は、監視センタから受け取った鍵データを記憶する。
【００６８】
送受信部１６は、無線や携帯電話の機能を一体化し、監視センタとの間の通信手段として利用するとともに鍵データの受信も行なう。監視センタとの通信の際、認証用データの送受信もここで行なう。
【００６９】
施解錠信号出力部１７は、契約先に設置された錠を施解錠させるために設けられたカードリーダ等の入力手段に対して施解錠信号を送信し、錠を施解錠する。
なお、前記施解錠信号は、直接施解錠するために用いられる信号に限らず、施解錠の際に用いられる識別情報でもよい。
【００７０】
例えば、入力手段が非接触カードを読み取るカードリーダの場合、非接触カードからカードリーダに対して施解錠用の識別情報が送信され、錠の制御装置において識別情報が確認されると施解錠が行なわれる。施解錠信号出力部は、非接触カード等に記憶されカードリーダに送信される識別情報と同様の情報をカードリーダに送信することにより、錠を施解錠する。
【００７１】
なお、入力手段が暗証番号を入力するテンキーの場合、携帯端末の表示部１１に当該暗証

番号を表示させ、警備員等がその暗証番号を入力すればよい。
【００７２】
耐タンパ手段１８は、携帯端末１が分解されるなどして不正に鍵データが奪われるのを防止するため、携帯端末１が分解されたことを検知すると、鍵データを消去する。また、鍵データ以外に不正入手されたくない情報がある場合、それらも同時に消去するようにしてもよい。
【００７３】
入出力部１９は携帯電話２０ａ，無線機２０ｂ等の他の無線機２０が接続されて信号の授受を行なう。
【００７４】
より高いレベルのセキュリティが求められる場合において、携帯端末が正規のものであることを確認するための認証を行なう場合、認証と施解錠信号の出力を一連のものとして行ない、認証により正規の携帯端末であることが認められた上で施解錠が行なわれるようにする。
【００７５】
なお、送受信部１６（入出力部）および施解錠信号出力部１７は共用してもよい。
その他、携帯端末１は電源を供給するバッテリ（図示せず）を備える。後付け電気錠を用いる場合、電気錠装置を駆動させるための電源を供給するようにしてもよい。
【００７６】
本発明による携帯端末１は、監視センタとの通信により、監視センタから鍵データを受信する。このとき、以下に示す通信手段のいずれかを用いればよい。
【００７７】
無線機との接続
監視センタと警備員（保守要員）との間で、監視センタからの指示や警備員からの報告を行なう際、無線が利用されている場合は、無線機２０ｂと携帯端末２とを接続ケーブルなどを利用して接続し、鍵データの受信等を行なえばよい。
【００７８】
携帯電話、ＰＨＳとの接続
監視センタと警備員（保守要員）との間で、監視センタからの指示や警備員からの報告を行なう際、携帯電話やＰＨＳ２０ａが利用されている場合は、携帯電話やＰＨＳ２０ａと携帯端末とを接続ケーブルなどを利用して接続し、鍵データの受信等を行なえばよい。
【００７９】
無線機、携帯電話、ＰＨＳ機能を携帯端末に設ける
図５（ａ）の携帯端末１のように、携帯端末に無線機、携帯電話、ＰＨＳ等による通信機能を持たせ、監視センタからの指示や警備員からの報告に利用するとともに、鍵データの受信を行なうことができる。
【００８０】
なお、携帯電話やＰＨＳの機能を持たせた場合、監視センタから携帯端末を呼び出す際は電話番号により携帯端末を指定でき、携帯端末から監視センタを呼び出した際は発信者番号通知を利用して携帯端末を特定できる。
【００８１】
したがって、この場合は、監視センタから鍵データを送信する際、正規の携帯端末であるか否かを確認するための認証を省略することもできる。
【００８２】
暗号化コードを携帯端末に入力
携帯電話や無線を利用して監視センタから警備員に指示を与える際、監視センタから鍵データとして、暗号化コード（例えば、１０桁程度の数列）を伝え、警備員はその暗号化コードを携帯端末に入力し、携帯端末で復号して鍵データとして利用する。
【００８３】
なお、この暗号化コードを生成する際、日付などのパラメータを利用して日によって異な

る暗号化コードが生成されるようにし、ある錠を施解錠する鍵データを暗号化した暗号化コードが同一とならないようにすることが好ましい。

【００８４】

また、鍵コードを送る際の認証においても、同様の暗号化－複合アルゴリズムを利用し、警備員や携帯端末の識別番号を暗号化した暗号化コードを監視センタに伝え、監視センタにおいて複合し、確認をとるようにしてもよい。

【００８５】

この場合、監視センタと警備員との間の通信に使われていた無線機等をそのまま利用できるというメリットがある。

【００８６】

携帯端末を使用する者の認証について

携帯端末を使用する者が正当な権限を与えられた者であるか否かを確認する方法として、以下の方法が考えられる。

【００８７】

（ａ）携帯端末において認証

監視センタから鍵データを受信する際、携帯端末により錠を施解錠する際、予め携帯端末に記憶させた比較対象とする情報と、携帯端末を使用する者が所有するＩＤカードに記憶された情報とを比較し、認証を行なう。

【００８８】

（ｂ）監視センタにおいて認証

監視センタから鍵データを受信する際、携帯端末により読み取られた、使用者のＩＤカードに記憶された情報、使用者の指紋などの生体情報を監視センタに送信し、監視センタにおいて予め記憶された比較対象とする情報と比較し、認証を行なう。

【００８９】

携帯端末により錠を施解錠する場合、鍵データを受信する場合と同様に監視センタにおいて認証してもよいが、施解錠の都度、監視センタと通信を行なうので通信費が嵩む。また、建物内において携帯電話やＰＨＳが使用できず、認証を行なえない可能性がある。

【００９０】

そこで携帯端末により錠を施解錠する場合は、鍵データを受信する際に認証を行なった使用者と同一人物であるか否かを確認すればよい。そのため、携帯端末は鍵データを受信する際の認証に使われた使用者の情報を記憶しておき、錠を施解錠する際、記憶された情報と使用者の情報とを比較照合する。

【００９１】

携帯端末の認証について

監視センタから鍵データを受け取る際、携帯端末が正規のものであることを確認するための認証方法としては、以下の方法がある。

【００９２】

携帯端末には予め識別コードを割り当てておく。また、監視センタでは、携帯端末に割り当てられたそれぞれの識別コードを登録しておく。

【００９３】

携帯端末は、鍵データを受け取るために監視センタと通信する際、自己の識別コードを監視センタに送信し、監視センタでは送られてきた識別コードと予め登録された識別コードとを比較照合し、正規の携帯端末であることを確認する。

【００９４】

このとき同時に、携帯端末の使用者が正当な権限を与えられた者であることの認証を行なってもよい。

【００９５】

また、監視センタでは、予め担当地区、警備員（保守要員）、携帯端末の対応関係を登録したデータベースを準備しておき、鍵データを渡す際の認証において、対象となる契約先が所在する地区、携帯端末の使用者、携帯端末の対応関係が正しいことを確認することに

より、さらに信頼性の高い認証を行なうようにしてもよい。

【００９６】

監視センタは、正規の携帯端末であることが確認されると、携帯端末に鍵データを送信する。このとき送信する鍵データは、これから向かう契約先において必要となる鍵のデータのみとする。なお、契約先において複数の鍵データを必要とする場合は、複数の鍵データを送信する。

【００９７】

なお、携帯端末と監視センタとの間の通信方法によっては、携帯端末が正規のものであることの確認を簡略化できる。

【００９８】

携帯端末１のように携帯端末に携帯電話やＰＨＳの機能を持たせた場合、監視センタから携帯端末を呼び出す際、電話番号により対象となる携帯端末を指定でき、携帯端末から監視センタを呼び出した際、監視センタでは発信者番号通知を利用して携帯端末を特定できる。

【００９９】

したがって、これらを利用することにより、携帯端末が正規のものであることを確認でき、識別コード等による確認を行なわなくてもよい。

携帯端末と契約先錠との認証について（後付け電気錠の場合）

既存のシリンダ錠のような機械式錠に電気的に制御を行なえるようにした制御装置を追加して取り付けた、所謂、「後付け電気錠」を用いる場合、外部から給電して施解錠信号を入力するだけで施解錠できるようにすると、任意のバッテリを接続し、任意の制御装置から施解錠信号を入力すると誰でも施解錠できることになる。

【０１００】

これを防ぐため、後付け電気錠を用いる場合は、電気錠と携帯端末との間で認証を行なうことにより、正規の携帯端末であることを確認する必要がある。

【０１０１】

図７に、公開鍵を利用して認証を行なう場合の例を示す。

【０１０２】

電気錠の制御装置３０には、予め任意の認証局Ａから発行された公開鍵（１）と秘密鍵（１）、鍵データ（錠ID 123）を登録しておく。また、携帯端末１には、予め任意の認証局Ａから発行された公開鍵（２）と秘密鍵（２）を登録しておく。認証は以下の手順により行なう。

（１）異常事態の検知や保全作業などにより契約先の建物に入館する場合、監視センタ１００と携帯端末１との間で認証が行なわれた後、監視センタ１００から公開鍵(２)で暗号化された鍵データ（錠ID 123）が携帯端末１に送信される(S1)。

（２）電気錠の制御装置３０と携帯端末１との間で予め登録された公開鍵（１），（２）を交換し、任意の認証局Ａに認められたものであることを互いに確認する（Ｓ２）。

（３）電気錠の制御装置３０から携帯端末１に対して、（Ｓ２）で受け取った公開鍵（２）で暗号化した鍵データ（錠ID 123）が書かれた文書を送信し署名を要求する（Ｓ３）。

（４）携帯端末１は、（Ｓ３）で受け取った文書を自らの秘密鍵（２）で復号し、（Ｓ１）で監視センタ１００から送信された鍵データと、（Ｓ３）で電気錠の制御装置３０から送信された鍵データを比較する（Ｓ４）。

（５）鍵データが等しい場合、携帯端末１は（Ｓ４）で復号した文書にデジタル署名する（Ｓ５）。

（６）携帯端末１から電気錠の制御装置３０に対して、（Ｓ５）でデジタル署名された文書を（Ｓ２）で受け取った公開鍵（１）で暗号化し送信する（Ｓ６）。

（７）電気錠の制御装置３０は、署名を確認後、施解錠する（Ｓ７）。

【０１０３】

図７に示す例によれば、厳重な認証により他人に悪用される恐れがほとんどなく、重要施設などにおいても利用できる高い信頼性を得ることができる。

【０１０４】
しかしながら、一般の建物において利用する場合、必要以上に厳重になりすぎて、管理上、負担となる恐れがある。
【０１０５】
本発明による携帯端末１は、監視センタ１００から鍵データを送信されなければ利用できないこと、監視センタ１００から鍵データを送信する際、携帯端末１が正規のものであることおよび携帯端末１の使用者が正当な権限を与えられた者であることを確認すること、携帯端末１は鍵データを不正入手されないための対策を施すことなどから、認証の一部を簡略化しても十分な信頼性を得ることができる。
図８に、図７の例において認証の一部を簡略化した場合の例を示す。
【０１０６】
電気錠の制御装置３０には、予め任意の認証局Ａから発行された公開鍵１と秘密鍵１、鍵データ（錠ID 123）を登録しておく。
（１）異常事態の検知や保全作業などにより契約先の建物に入館する場合、監視センタと携帯端末との間で認証が行なわれた後、監視センタから公開鍵（１）で暗号化された錠前情報（錠ID 123）が携帯端末１に送信される（Ｓ１１）。
（２）携帯端末１は（Ｓ１０）で監視センタ１００から受信した暗号化された鍵データ（錠ID 123）と、施解錠信号を電気錠の制御装置３０に送信する（Ｓ１２）。
（３）電気錠の制御装置３０は、（Ｓ１２）で受け取った暗号化された鍵データ（錠ID 123）を秘密鍵（１）で復号し、鍵データ（錠ID 123）を比較する（Ｓ１３）。
（４）鍵データの一致を確認後、（Ｓ１２）で受け取った施解錠信号により施解錠する（Ｓ１４）。
【０１０７】
携帯端末に記憶される鍵データの扱いについて
携帯端末１には監視センタ１００から受け取った鍵データを記憶するが、携帯端末１が盗難や紛失にあっても、鍵データの漏洩による被害を最小限に抑えるため、以下に示すような対策を行ない、携帯端末１には最低限の数の鍵データを必要とされる間だけ記憶するようにしておく。
（１）監視センタ１００から新たな鍵データを受け取ると、過去に受け取った鍵データを消去する。
（２）携帯端末１に設けられた消去手段の操作により消去する（警備員による異常確認や事態の収拾などが終わり、契約先建物から警備員が退出した（入口扉を施錠した）後に消去すればよい。）。
（３）監視センタ１００から鍵データを受信してから一定時間有効とし、消去する。鍵データの中に有効期間を指定する情報を含ませておく。
（４）携帯端末１内にタンパスイッチを設けておき、分解されるなどすると鍵データを消去する。
（５）解錠が１回行なわれると鍵データを消去（または解錠操作を禁止）する。
（６）解錠が行なわれてから施錠操作が行なわれるまで有効にする。
（７）監視センタ１００に作業終了の連絡を入れた際、監視センタ１００からの操作（監視センタから携帯端末に消去命令を送信）により消去する。
【０１０８】
なお、鍵データの扱いに関し、鍵データの消去などにより施錠、解錠操作双方を禁止してもよいが、解錠操作のみ禁止するようにしてもよい。
これは、不正に解錠されることにより悪用される可能性はあっても、不正に施錠されることにより悪用される可能性は極めて低いからである。
【０１０９】
鍵データの内訳について
鍵データの内訳として想定されるものを、以下に示す。以下に示す情報を必要に応じて選択し、利用する。

（１）識別情報
錠を施解錠する際、錠の側の制御装置において、照合のために利用される情報。
【０１１０】
非接触カードから送信される識別情報、暗証番号、個人のＩＤコードなど、携帯端末以外を利用して錠を施解錠する場合に、カードリーダ等に送られる情報と同様の情報である。
（２）施解錠の対象となる錠の錠前情報（ＩＤ）
施解錠を行なう際、対象となる錠が正しいか否かを確認する場合に使用する。
（３）錠の種類（異なる種類の錠を施解錠する場合に使用）
対象となる錠に応じて、認証のためのデータや施解錠信号の出力方法を変更するために使用する。この情報に基づいて無線で送受信、暗証番号等を表示部に表示、任意の入出力端子を介して信号を入出力、などを切り替える。
（４）鍵データの消去条件（有効回数、有効期間など、状況に応じて消去条件を変更する場合に使用）
施解錠の対象が建物の入口扉であれば、１度だけ施解錠できれば十分であるが、各階の入口扉で共通の鍵が必要である場合は、複数回施解錠しなければならない。このような場合は回数ではなく、必要な作業時間をもとに有効期間（例えば２時間）を定めておけばよい。
（５）錠の名称など（複数の錠を施解錠する場合、警備員が施解錠する錠に応じて施解錠信号を選択する場合に使用；「建物入口扉」、「○階入口扉」などの名称）
携帯端末により複数の錠を施解錠する場合、警備員はどの錠を施解錠するのかを選択し指定しなければならない。その際に利用するための、錠の名称である。
シリンダ錠が用いられている契約先について
テナントビル等において、出入口扉に電気錠が設けられカードや暗証番号により施解錠している場合は、本発明による携帯端末を容易に導入することができる。
【０１１１】
ところが、出入口扉にシリンダ錠が用いられている場合や、テナントビル等において、建物の出入口扉は暗証番号やカードにより施解錠できるものの、個々のテナントの扉にはシリンダ錠が用いられている場合などは、本発明による携帯端末により直接、それらの扉を施解錠することはできない。
【０１１２】
このような場合には、以下に示すような構成を付加するなどして対応する。
（１）鍵保管箱を設置する。
【０１１３】
鍵保管箱を設置し、シリンダ錠を施解錠するための鍵を鍵保管箱に収納する。
鍵保管箱の設置場所は、建物の入口扉がシリンダ錠であれば建物外部、建物内部にある各部屋の扉だけがシリンダ錠の場合は建物内部の入口付近に設置するようにすればよい。
【０１１４】
鍵保管箱はカードや暗証番号などにより鍵収納部を開閉し、鍵収納部に保管された鍵を取り出せるようになっている。警備員等はカードや暗証番号を利用するかわりに携帯端末を利用して鍵保管箱を開閉し、鍵を取り出せばよい。
【０１１５】
この場合、お客様の側では従来のシリンダ錠を施解錠するために用いていた鍵をそのまま利用できるというメリットがある。
【０１１６】
なお、鍵保管箱について、警備員だけが利用するのではなく、お客様も利用できるようにし、お客様は自分の部屋の鍵を鍵保管箱の収納し、カードや暗証番号を利用して鍵を取り出し、利用するようにしてもよい。
（２）出入口扉の錠を電気錠に交換する。
【０１１７】
出入口扉の錠を電気錠に交換する場合、電気錠の設置に多少費用はかかるものの、シリン

ダ錠の場合に発生していたピッキングによる不正解錠の恐れがなくなるため、防犯性能が大幅に向上する。

【０１１８】

なお、テナントビル等においては、建物入口のみを電気錠に変更し、建物内部は鍵保管箱を設置して各テナントの出入口等を施解錠するための鍵を鍵保管箱に収納するようにしてもよい。

（３）出入口扉の錠に電気錠を追加設置する。

【０１１９】

前記電気錠を設置する場合の問題として、設置費用が高い点があげられる。

【０１２０】

したがって、金銭的に余裕がある契約先や重要施設以外においては、容易に設置することができなかった。

【０１２１】

電気錠を追加設置する場合、大掛かりな配線工事を施したり、電気錠を駆動させるために新たに電源装置を設けたりする必要があり、工事費などが高くなっていた。

【０１２２】

そこで、シリンダ錠の部分に電気錠を追加設置し、警備員や保守要員が施解錠する場合は電気錠により施解錠するように変更する。契約先の者が施解錠する場合は、従来の鍵をそのまま利用して施解錠する。

【０１２３】

追加設置する電気錠は、常時電源を供給しておくのではなく、警備員等が携帯するバッテリから電源供給を受けたときに有効となり、携帯端末からの信号により施解錠する。大掛かりな配線工事等を無くし、設置費用を低減させる。

後付け電気錠の構造について

前述した後付け電気錠は、既にシリンダ錠が用いられている契約先においても、携帯端末による施解錠を可能にするため、シリンダ錠を電気的に制御するための制御装置を付加して電気錠と同等の機能を持たせたものである。この後付け電気錠について、以下、図９乃至図１３に基づいて説明する。

【０１２４】

先ず図９を参照すると、本発明による後付け電気錠５０は、シリンダ錠９０に付加して取り付けられるもので、大きく分けると給電端子６０、制御部７０、駆動部８０により構成される。

【０１２５】

給電端子６０は、制御部７０および駆動部８０を機能させるための電源を供給するための端子であり、警備員または保守要員がバッテリ２００を接続し、電力を供給する。

【０１２６】

制御部７０は、給電部６０より供給された電力によって動作し、駆動部８０を制御して錠を施解錠させる。このとき、携帯端末１との間で認証などを行ない、不正な施解錠が行なわれないようにする。

【０１２７】

駆動部８０は、後述するように、モータとリンク機構からなり、制御部７０の制御によりモータを駆動し、リンク機構を介してシリンダ錠９０のシリンダを回転させることにより錠を施解錠する。

【０１２８】

なお、契約先の者は、従来とおりの鍵を使用して錠を施解錠する。

【０１２９】

ここで、後付け電気錠の詳細について図１０～図１３に基づいて説明する。図１０は、扉２００にシリンダ錠９０と後付け電気錠５０が取り付けられた状態の概略図を示す。シリンダ錠９０は、扉２００を貫通する回転軸９１の両端に取り付けられた外部ドアノブ９２ａ及び内部ドアノブ９２ｂと、回転軸９１の回転により扉２００の端面より出入りするデ

ッドボルト９３を有する。外部ドアノブ９２ａは内部に鍵が挿入されるシリンダ部９３を有する。回転軸９１はシリンダ部９４に挿入される鍵９５、又は内部ドアノブ９２ｂを回転操作することにより回転軸９１を回転させてデッドボルト９３の出入りを行なわせ、施錠状態と解錠状態とするものである。

【０１３０】

後付け電気錠５０は扉２００の内側に装着され、駆動部８０は給電端子６０から供給される電力により制御部７０介して駆動され、駆動部８０の駆動によりシリンダ錠９０の回転軸９１を回転させて施解錠を行なう。

【０１３１】

図１１、図１２は、後付け電気錠駆動部８０の駆動機構を説明するものである。駆動部８０は、モータ８１とギア８２，８３を介して駆動されるリンク機構８４からなる。

【０１３２】

モータ８１の回転は、ギア８２を介してギア８３に伝達される。ギア８３にはスリット８３ａが設けられており、そのスリット８３ａにはリンク機構の一方の端部に設けられたフック８４ａが係合するようにされている。そして、ギア８３が回転してもフック８４ａに当接するまではリンク機構８４に力が伝達されないようになっている。

【０１３３】

ギア８３がフック８４ａに当接するまで回転した後さらに回転すると、リンク機構８４に力が伝わり図示するようにリンク機構８４が動き、リンク機構８４の他方の端部に連結された回転軸９１が回転される。

【０１３４】

図１２は、モータ８１の回転によって回転軸９１が回転された状態（点線）を示している。このようにしてモータ８１の力を使って回転軸９１を回転させ、施解錠することができる。

【０１３５】

ところで、モータの力を単に回転軸に伝えるだけであれば、スリット８３ａは不要である。

【０１３６】

しかしながら、モータ８１と回転軸９１が連結された状態であると、後付け電気錠を用いずに鍵を使用して施解錠しようとする場合に、回転軸とモータを同時に回すことになるため、大きな負荷がかかってしまう。スリット８３ａは鍵などを使って施解錠する場合に負荷がかからないようするために設けたもので、リンク機構とギア機構との間で力の伝達を遮断する遊びとして機能するものである。図１３は、このスリット８３ａの働きについて説明するための図である。なお、上記の負荷がかかるのを避けるため、後付け電気錠５０により施解錠する場合、施解錠した後（図１３▲１▼）、スリット８３ａが設けられている分だけギア２を逆転させるようにしておく（図13▲２▼）。

【０１３７】

この状態において、鍵などにより施解錠した場合でも、回転軸の回転がギア２に伝わらないため、モータによる負荷がかからないこととなる（図１３▲３▼）。

【０１３８】

携帯端末に汎用性を持たせるための手段について

現在、建物等の入口扉には様々な種類の錠が用いられており、それらの錠を施解錠する方法も様々である。現在使われている主な方法としては、鍵を用いるもの、暗証番号を用いるもの、磁気カードや非接触カードなどのＩＤ（施解錠用）カードを用いるもの等がある。また、今後は従来のカードと比較してセキュリティ性の高いＩＣカードが利用されることも予想される。

【０１３９】

警備員が保管する鍵の削減および鍵の受け渡しを不要にするという観点からすれば、理想的には、携帯端末により全ての錠を施解錠できるようにすればよい。そのようにした場合、警備員は携帯端末のみを持てばよいこととなる。

【０１４０】
これを実現するには、全ての錠を携帯端末で施解錠できるものに変更するか、携帯端末から出力する施解錠信号を各種の錠に適合する形式で出力できるようにすればよい。
【０１４１】
ここでは、携帯端末から出力する施解錠信号を各種の錠に適合させた形式で出力する場合について、説明する。
【０１４２】
施解錠信号を各種の錠に適合させた形式で出力するには、携帯端末に異なる形式で信号を出力するための機能を設けるか、携帯端末にアダプタを接続して対応する。
【０１４３】
例えば、非接触カードにより施解錠する錠に対しては、無線の送受信手段により施解錠のための信号を入出力し、暗証番号により施解錠する錠に対しては、携帯端末の表示部に暗証番号を表示させるようにすればよい。
【０１４４】
磁気カードにより施解錠する錠の場合は、カード状のアダプタを携帯端末に接続し、磁気カードリーダに識別情報を直接送り込むか、携帯端末に磁気カードライタを接続し、磁気カードに識別情報を書き込むことにより磁気カードを作り、その磁気カードを利用して施解錠するようにしてもよい。
【０１４５】
ただし、このようにして作られた磁気カードが悪用されないよう、携帯端末は作り出した磁気カードの情報を記憶しておき、磁気カードを作ってから所定時間以内に当該磁気カードを磁気カードライタに読み込ませて識別情報を消去し（所定時間以内に当該磁気カードが読み込まれなかった場合は異常ありの旨を監視センタに報知するか、携帯端末を使用不能にするなどすればよい）、前回作られた磁気カードが読み込まれた場合のみ、当該磁気カードに識別情報等を上書きすることにより新たな磁気カードを作り出すようにすればよい。
【０１４６】
また、新たな種類の錠に対応できるよう、監視センタから送信される錠データには、施解錠信号を出力する際のデータフォーマット、出力方法（無線等）を指定する情報も含まれるようにし、その情報に基づき、それぞれの錠に対応した形式で施解錠信号を出力すればよい。
【０１４７】
機械警備システムの警備／警備解除の設定について
本発明による携帯端末を使用するのは、警備員または保守要員が施錠された契約先建物に入館する場合である。
【０１４８】
この場合、機械警備システムが用いられている施設にあっては、機械警備システムが警備状態に設定されているため、警備員または保守要員は警備解除するか、警備員等が入館していることを示すモードである巡回モードに設定しなければならない。
【０１４９】
機械警備システムの設定は、磁気カードや非接触カード等のＩＤカードや暗証番号により行なわれており、契約先建物の錠を施解錠する場合に用いられる手段と同様の手段が用いられている。
【０１５０】
そこで、本発明による携帯端末を利用し、施解錠信号の代わりに警備／警備解除信号を送信し、警備／警備解除を設定するようにしてもよい。
【０１５１】
携帯端末の利用者について
本発明による携帯端末について、警備会社の警備員や保守要員が利用する場合を例に説明したが、携帯端末の利用者はこれに限らず、建物の空調、配電、配水等を管理する設備業

者が携帯し、設備異常が発生した場合に携帯端末を利用して建物に入館するようにしたり、建物の清掃を受け持つ業者が携帯して夜間や早朝、清掃のため建物に入館する際に利用したりしてもよい。

【０１５２】

【発明の効果】

本発明によれば、以下に述べるように種々の効果を得ることができる。

【０１５３】

マスターキー機能を有する携帯端末を導入することにより、警備員が保管しなければならない鍵の数を大幅に削減し、管理上の負担を軽減できる。

【０１５４】

マスターキー機能を有する携帯端末の導入により、従来のように鍵の受け渡しが不要となるので、鍵の受け渡しに伴う煩わしい手続きが不要であるとともに、速やかに現場に向かい事態の収拾および被害の拡大防止を行なうことができる。

マスターキー機能を有する携帯端末は、マスターキーのように複数の錠を施解錠できるものの、そのために利用される契約先の鍵データは、必要な場合に必要な分だけ監視センタから送信するため、万が一、携帯端末が盗難や紛失などしても被害を最小限にとどめることができる。

【０１５５】

鍵データとして監視センタから受け取った暗号化コードを携帯端末に入力して施解錠信号を生成できるようにしたことにより、従来、監視センタと警備員または保全要員との間の連絡に利用されていた携帯電話や無線機をそのまま利用でき、既存の運用システムを無駄にすることなく携帯端末を導入できる。

【０１５６】

携帯端末の使用者は、認証を行なうことにより正当な権限を与えられた者であることが確認され、また、携帯端末も認証により正規の携帯端末であることが確認されるので、正当な権限を与えられた者以外は携帯端末を利用できず、悪用されるのを防ぐことができる。

【０１５７】

マスターキー機能を有する携帯端末は、施解錠する対象となる錠（のカードリーダ等の入力手段）に対応する施解錠信号を出力し、あるいは施解錠する対象となる錠に対応する施解錠信号を出力できるアダプタを接続することにより、異なる種類の錠を携帯端末により施解錠することができる。

【０１５８】

シリンダ錠に用いられているマスターキーと比較すると、本発明のマスターキー機能を有する携帯端末は容易に複製できない。また、ハード的に同等の物が作られたとしても、鍵データがなければ使用できない。携帯端末に鍵データを送るのは、監視センタから警備員に派遣の指示を行なう場合に限られ、また、認証により身分を確認することから、不正入手は困難である。したがって、非常に安全性の高いキーといえる。

【０１５９】

本発明による電気錠は、携帯端末より出力される施解錠信号により動作し、携帯端末の機能を有効に利用することが可能となる。

【０１６０】

本発明による電気錠は、駆動部のリンク機構とギア機構との間に遊びを設けたことにより、モータを使わず、鍵などにより施解錠する場合は、モータによる負荷がかからずに施解錠できる。

【図面の簡単な説明】

【図１】警備員が鍵の授受を行なった後に現場に向かう従来例を説明する図である。

【図２】警備員が鍵データを受け取る手順を示す図である。

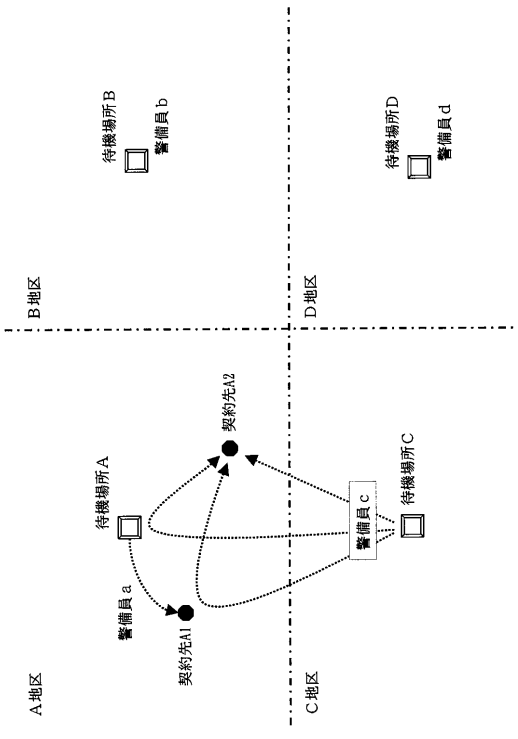
【図３】保守要員が鍵データを受け取る手順を示す図である。

【図４】警備員・保守要員が鍵データを受け取る他の手順を示す図である。

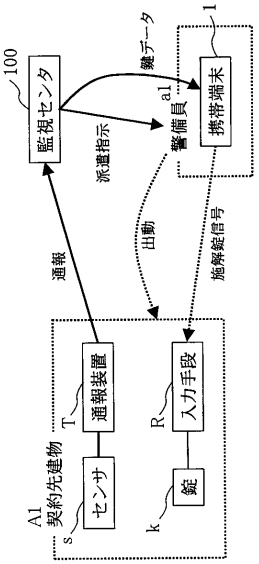
【図５】本発明による携帯端末の構成を示すブロック図である。

【図６】本発明による携帯端末の概観図である。
【図７】鍵データを利用して施解錠する場合の認証手順を示す図である。
【図８】鍵データを利用して施解錠する場合の他の認証手順を示す図である。
【図９】後付け電気錠の構成を示す図である。
【図１０】後付け電気錠の取付構造を示す図である。
【図１１】後付け電気錠の駆動機構の動作説明図である。
【図１２】後付け電気錠の駆動機構の動作説明図である
【図１３】後付け電気錠の施解錠動作の説明図である。
【符号の説明】
１、２　携帯端末
１１　表示部
１２　操作部
１３　認証部
１４　制御部
１５　記憶部
１６　送受信部
１７　施解錠信号出力部
１８　耐タンパ手段
３０　電気錠の制御装置
１００　監視センタ

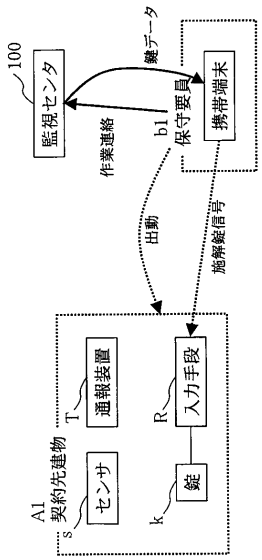
【図１】



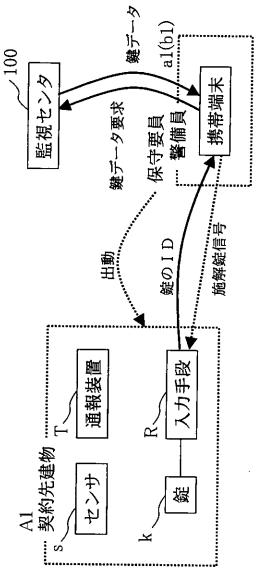
【図２】



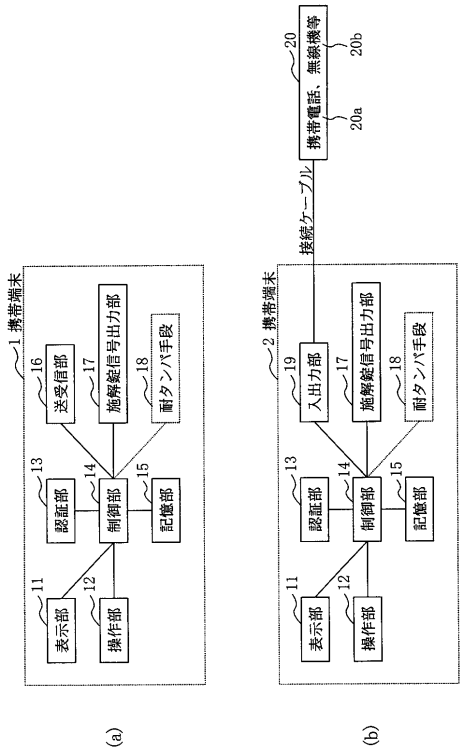
【図３】


100
監視センタ
鍵データ
作業連絡
b1
保守要員
携帯端末
出動
施解錠信号
A1
契約先建物
センサ
s
T
通報装置
R
入力手段
k
錠

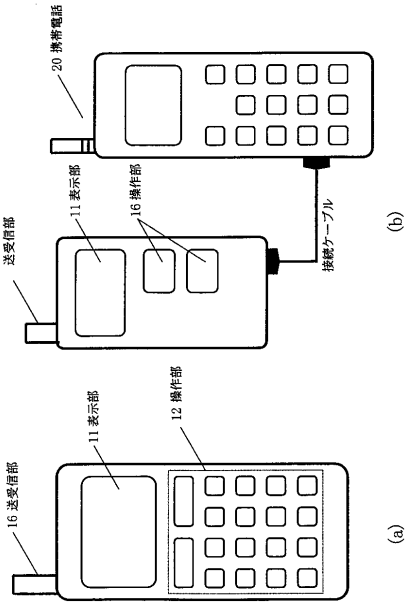
【図４】


100
監視センタ
鍵データ
a1(b1)
鍵データ要求
保守要員
警備員
携帯端末
出動
錠のＩＤ
施解錠信号
A1
契約先建物
センサ
s
T
通報装置
R
入力手段
k
錠

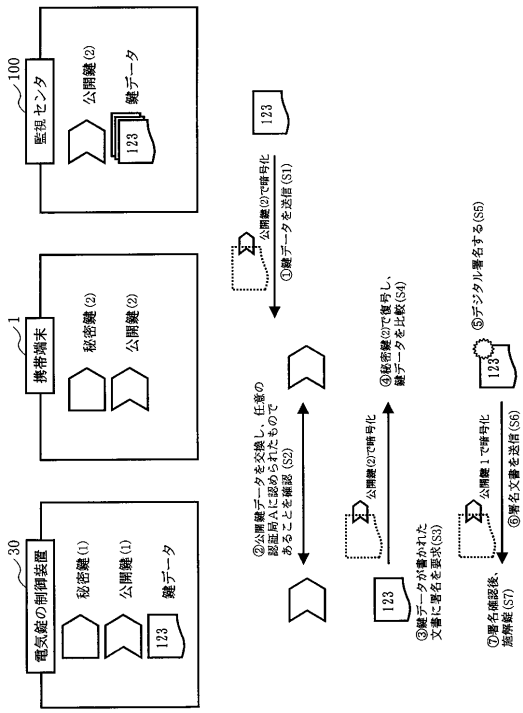
【図５】


1 携帯端末
11 表示部
12 操作部
13 認証部
14 制御部
15 記憶部
16 送受信部
17 施解錠信号出力部
18 耐タンパ手段
(a)
2 携帯端末
11 表示部
12 操作部
13 認証部
14 制御部
15 記憶部
17 施解錠信号出力部
18 耐タンパ手段
19 入出力部
接続ケーブル
20 携帯電話、無線機等
20a
20b
(b)

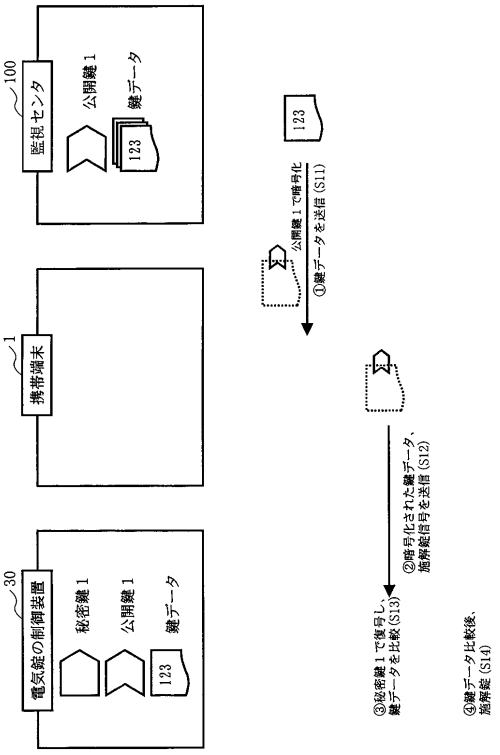
【図６】


16 送受信部
11 表示部
12 操作部
(a)
20 携帯電話
送受信部
11 表示部
16 操作部
接続ケーブル
(b)

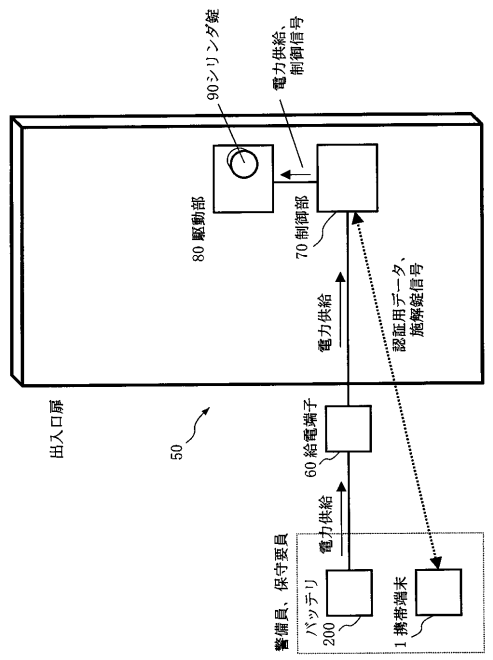
【図７】


100
監視センタ
公開鍵(2)
鍵データ
123
1
携帯端末
秘密鍵(2)
公開鍵(2)
30
電気錠の制御装置
秘密鍵(1)
公開鍵(1)
鍵データ
123
①鍵データを送信(S1)
公開鍵(2)で暗号化
②公開鍵データを交換し、任意の認証局Aに認められたものであることを確認(S2)
③鍵データが書かれた文書に署名を要求(S3)
公開鍵(2)で暗号化
④秘密鍵(2)で復号し、鍵データを比較(S4)
⑤デジタル署名する(S5)
⑥署名文書を送信(S6)
公開鍵1で暗号化
⑦署名確認後、施解錠(S7)

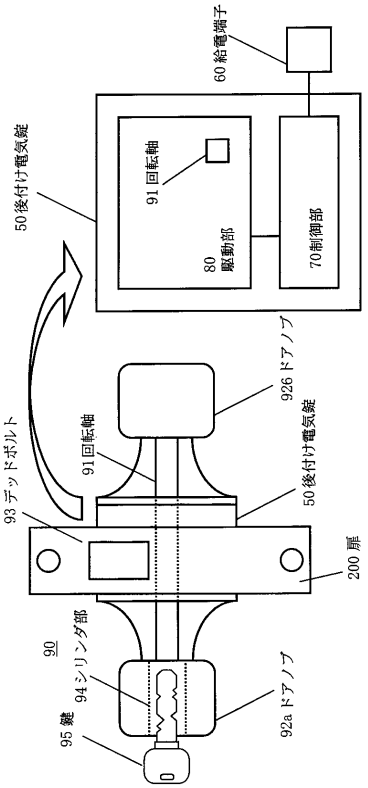
【図８】


100
監視センタ
公開鍵1
鍵データ
123
1
携帯端末
30
電気錠の制御装置
秘密鍵1
公開鍵1
鍵データ
123
①鍵データを送信(S11)
公開鍵1で暗号化
②暗号化された鍵データ、施解錠信号を送信(S12)
③秘密鍵1で復号し、鍵データを比較(S13)
④鍵データ比較後、施解錠(S14)

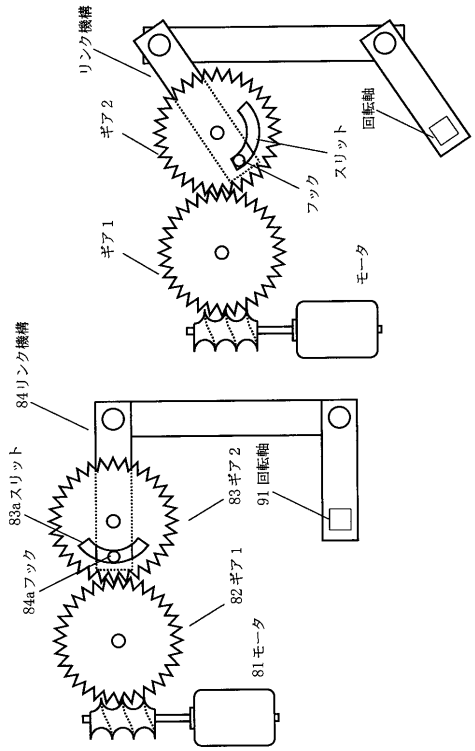
【図９】


90シリンダ錠
電力供給、制御信号
80 駆動部
70 制御部
電力供給
認証用データ、施解錠信号
出入口扉
50
60 給電端子
電力供給
警備員、保守要員
バッテリ
200
1 携帯端末

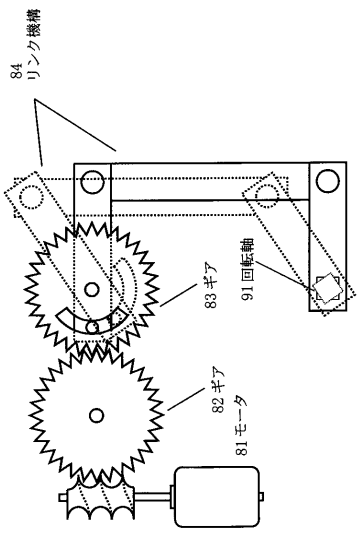
【図１０】


60 給電端子
50後付け電気錠
91 回転軸
80 駆動部
70制御部
926 ドアノブ
93 デッドボルト
91回転軸
50 後付け電気錠
200 扉
90
94シリンダ部
95 鍵
92a ドアノブ

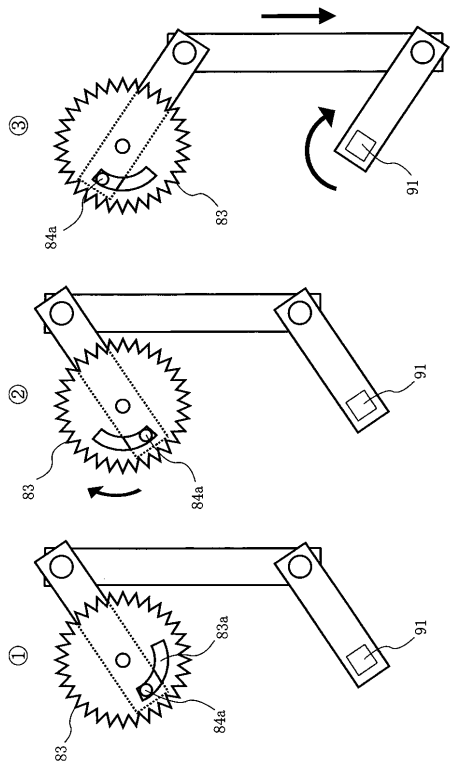
【図１１】


リンク機構
ギア２
スリット
回転軸
フック
ギア１
モータ
84リンク機構
83aスリット
83ギア２
91回転軸
84aフック
82ギア１
81モータ

【図１２】


84
リンク機構
83ギア
91回転軸
82ギア
81モータ

【図１３】


③
84a
83
91
②
83
84a
91
①
83a
84a
83
91

フロントページの続き

(51)Int.Cl.	FI	
	E05B 49/00	S
	E05B 19/00	E
	E05B 35/12	B
	E05B 47/00	J

(56)参考文献 特開平１０－２９２６８９（ＪＰ，Ａ）
特開平０５－２３３８９６（ＪＰ，Ａ）
特開平０８－１８４２３３（ＪＰ，Ａ）
特開平１１－０７１９５０（ＪＰ，Ａ）
特開２０００－０７６４５１（ＪＰ，Ａ）
特開平０１－２５０５７９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
E05B 49/00
E05B 19/00
E05B 35/12
E05B 47/00